

## COMMENTS

The enclosed is responsive to the Examiner's Office Action mailed on May 9, 2002. At the time the Examiner mailed the Office Action claims 1 through 59 were pending. In response, the Applicant has: 1) canceled claim 27 without prejudice; 2) amended claim 26; and, 3) added new claims 60 through 89. As such, claims 1 through 26 and 28 through 89 are pending. The applicant respectfully requests reconsideration of the present application and the allowance of claims 1 through 26 and 28 through 89.

The Examiner has rejected each of independent claims 1, 13, 29 and 42 under 35 USC 102(e) as being anticipated by U.S. Patent No. 6,257,486 B1 (hereinafter, "Teicher"). "To anticipate a claim, the reference must teach every element of the claim." MPEP 2131 The Applicant respectfully submits that Teicher fails to disclose each and every element of the Applicant's claims. In particular, note that each of independent claims recites three functional entities: 1) "a smart card"; 2) "a smart card enabler"; and, 3) "a smart card reader". As such, claims 1, 13, 29 and 42 are each directed to a smart card technology approach that involves each of these three functional entities.

Close examination of Teicher, however, reveals that Teicher only discloses a smart card approach that involves two functional entities as opposed to three functional entities. Better said, Teichner only discloses a smart card and a smart card reader and does not disclose a smart card enabler. As such, it is impossible for Teicher to disclose each and every one of the elements of Applicants claims. According to the teachings of Teicher, the smart card of Teicher performs personal identification number (PIN) authentication. Because

the smart card performs PIN identification, Teicher maintains that a more secure system results because sensitive PIN information never leaves the smart card which; in turn, makes “hacking” the smart card reader in an attempt to steal the PIN information much more difficult.

Figures 6 and 7 of Teicher along with the discussions provided on Column 5, line 59 through Column 6, line 34 and Column 7, line 55 through Column 8, line 52 of Teicher provide an overview of a prior art card authentication approach (wherein the smart card performs smart card authentication) over which Teicher sought to make an improvement. Column 8, lines 52 through 62 disclose the security vulnerability associated with the prior art approach. Here, Column 10, line 66 through Column 11, line 7 of Teicher provide the thrust of Teicher:

The present invention overcomes the above-discussed limitations of the prior art by providing a novel smart card-reader system, wherein the smart card performs the user authentication when presented to the reader, and is normally prevented from doing so when not presented to the reader. This is accomplished by providing an authentication module on the smart card for authenticating the user, which is normally disabled but which can be enabled by the reader when the smart card is presented to the reader.

Thus, as Teicher only involves the use of two functional entities to perform a smart card transaction (a smart card and a smart card reader), it is impossible for Teicher to disclose the three functional entities to perform a smart card

transaction as recited in Applicant's claims 1, 13, 29 and 42 (a smart card, a smart card reader and a smart card enabler). Therefore each of independent claims 1, 13, 29 and 42 are not anticipated by Teicher.

The Examiner also rejected independent claim 26 as being obvious over the combination of Teicher, U.S. Patent No. 6,070,795 (hereinafter, "Feiken") and Japanese Patent Application JP 8-187, 346 (hereinafter, Niiyama). "To establish a *prima facie* case of obviousness ... the prior art reference (or references when combined) must teach or suggest all the claim limitations." MPEP 2143. The Applicant respectfully submits that the combination of Tiecher, Feiken and Niiyama fail to disclose each and every element of independent claim 26. More specifically, as discussed, Teicher fails to disclose or suggest the use of three functional entities for the purpose of performing a smart card transaction; and, Feiken and Niiyama fail to cure the defect associated with Teicher. That is, neither Feiken nor Niiyama teach or suggest, alone or in combination, a three dimensional smart card system. As such, the combination of Teicher, Feiken, Niiyama do not teach or suggest "a smart card", "a smart card reader" and "a smart card enabler". As such, independent claim 26 is patentable over these references.

As the independent claims of the present application are allowable over Teicher and the combination of Teicher with Feiken and Niiyama, each of the dependent claims of the present application are patentable. As such, each of claims 1 through 26 and 28 through 89 are patentable over these references and the Applicant respectfully requests the allowance of same.

Applicants respectfully submit the present application is in condition for allowance. If the Examiner believes a telephone conference would expedite or assist in the allowance of the present application, the Examiner is invited to call Robert O'Rourke at (408) 720-8300.

Authorization is hereby given to charge our Deposit Account No. 02-2666 for any charges that may be due.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN



Date: 9/9/02

Robert B. O'Rourke  
Reg. No. 46,972

12400 Wilshire Boulevard  
Seventh Floor  
Los Angeles, CA 90025-1026  
(408) 720-8300

## **CLAIM AMENDMENTS SHOWING CHANGES**

Please cancel claim 27 without prejudice.

Please amend claim 26 as provided below.

26. (once amended) A method [for obtaining information stored in a smart card, the method], comprising:

recovering [from the smart card]information stored in a lost, damaged or destroyed smart card [if the information is incapable of being retrieved from the smart card using stored]by retrieving a copy of the information [in]from a memory, said memory part of a smart card enabler, said smart card designed to perform a transaction with a smart card reader.

Please add new claims 60 through 89.

60. (new) A smart card, comprising:

- a) a first interface through which communications with a smart card enabler are transported;
- b) a second interface through which communications with a smart card reader are transported;
- c) a memory resource to store an identification key, a transaction key and a transaction value; and
- d) a processing unit to:

- 1) send said identification key to said smart card enabler through said first interface;
- 2) send said transaction key to said smart card enabler through said first interface as a consequence of said smart card receiving a first enable signal from said smart card enabler, said first enable signal sent in response to said sending of said identification key;
- 3) send said transaction value to said smart card reader through said second interface in order to entertain a transaction, said transaction value being sent as a consequence of said smart card receiving a second enable signal from said smart card enabler, said second enable signal sent in response to said sending of said transaction key.

61. (new) The smart card of claim 60 wherein said second interface further comprises a contact interface.

62. (new) The smart card of claim 61 wherein said first interface further comprises an RF interface.

63. (new) The smart card of claim 60 wherein said first interface further comprises an RF interface.

64. (new) The smart card of claim 60 wherein said smart card further comprises an I/O interface coupled to said processing unit.

65. (new) The smart card of claim 64 wherein said I/O interface further comprises a key pad.
66. (new) The smart card of claim 64 wherein said I/O interface further comprises a display.
67. (new) The smart card of claim 60 wherein said smart card is further configured to create and store a new transaction key as a consequence of a new transaction value having been received from said smart card reader, said new transaction key stored into said memory resource, said new transaction value reflecting said transaction value less a cost for said transaction.
68. (new) The smart card of claim 67 wherein said smart card is further configured to send said new transaction key and said new transaction value to said smart card enabler.
69. (new) The smart card of claim 68 wherein said smart card is further configured to generate said new transaction key by generating a random number.
70. (new) An apparatus, comprising:
  - a smart card to perform a transaction with a smart card reader, said smart card enabled by a smart card enabler to said perform said transaction,

said smart card designed to send an identification key to said smart card enabler, said smart card designed to send a transaction key to said smart card enabler if said smart card receives a first enable signal from said smart card enabler in response to said sending of said identification key, said smart card designed to send a value to said smart card reader if said smart card receives a second enable signal from said smart card enabler in response to said sending of said transaction key, said smart card designed to store said identification key, said transaction key and said value.

71. (new) The apparatus of claim 70 wherein said smart card is further designed to send a second value to said smart card enabler in response to said transaction being performed with said smart card reader, said second value reflecting said value less the cost of said transaction.

72. (new) The apparatus of claim 71 wherein said smart card is further designed to send a new transaction key to said smart card enabler in response to said transaction being performed with said smart card reader.

73. (new) The apparatus of claim 72 wherein said new transaction key further comprises a randomly generated number.

74. (new) The apparatus of claim 70 wherein said smart card makes physical contact smart card reader to communicate with said smart card reader.

75. (new) The apparatus of claim 70 wherein said smart card wirelessly communicates to said smart card enabler.

76. (new) The apparatus of claim 70 wherein said smart card enabler is designed to send said first enable signal if said identification key matches a second identification key that is stored by said smart card enabler.

77. (new) The apparatus of claim 76 wherein said smart card enabler is designed to send said second enable signal if said transaction key matches a second transaction key that is stored by said smart card enabler.

78. (new) A method, comprising:

retrieving a saved identification key from within a smart card and sending said identification key from said smart card to a smart card enabler;

receiving at said smart card a first enable signal that was sent from said smart card enabler, said first enable signal responsive to said sending of said identification key;

retrieving a saved transaction key from within a smart card and sending said transaction key from said smart card to said smart card enabler;

receiving at said smart card a second enable signal that was sent from said smart card enabler, said second enable signal responsive to said sending of said transaction key; and

retrieving a saved value from within said smart card and sending said value from said smart card to a smart card reader, said value representing money available for one or more goods and/or services.

79. (new) The method of claim 78 further comprising deducting the cost of said goods and/or services from said value to create a second value.

80. (new) The method of claim 79 further comprising sending said second value from said smart card to said smart card enabler.

81. (new) The method of claim 80 further comprising sending a second transaction key along with said second value from said smart card to said smart card enabler.

82. (new) The method of claim 81 further comprising saving within said smart card both said second value and said second transaction key.

83. (new) The method of claim 82 wherein said second transaction key further comprises a randomly generated number, said method further comprising generating said second transaction key within said smart card prior to said sending of said second transaction key.

84. (new) The method of claim 78 further comprising, within said smart card enabler, comparing said identification key with a stored identification key and

sending said first enable signal because said identification key matchers said stored identification key.

85. (new) The method of claim 78 further comprising, within said smart card enabler, comparing said transaction key with a stored transaction key and sending said second enable signal because said transaction key matches said stored transaction key.

86. (new) A smart card, comprising:

first means for storing an identification key, a transaction key and a value, said value representing money available for one or more goods and/or services; second means for transmitting said identification key to a smart card enabler and for transmitting said transaction key to said smart card enabler, said transmitting said transaction key in response to a first enable signal having been received from a smart card enabler, said first enable signal having been sent in response to said transmitting of said identification key; and.

third means for transmitting said value to a smart card reader, said transmitting said value in response to a second enable signal having been received from said smart card enabler, said second enable signal having been sent in response to said transmitting of said transaction key.

87. (new) The smart card of claim 85 wherein said second means is also for transmitting a second value to said smart card enabler, said second value being said value deducted by the cost of said one or more goods and/or services.

88. (new) The smart card of claim 86 wherein said second means is also for transmitting, along with said second value, a second transaction key to said smart card enabler.

89. (new) The smart card of claim 86 wherein said first means is also for storing said second value and said second transaction key.